REMARKS/ARGUMENTS

Specification

Pages 1 and 2 of the specification have been amended to update the list of co-pending applications with USPTO application and granted serial numbers.

Claims

The Examiner rejected claims 1-5 and 7-17. By the present amendment, claims 1-5, 7-8, and 10-17 have been amended, and claim 9 has been cancelled. Therefore claims 1-5, 7-8, and 10-17 remain pending in the application.

Claim Rejections – 35 USC §103

Claims 1-5 and 7-17 were rejected under 35 U.S.C. 102(e) as being anticipated by Eldridge et al. (U.S. Patent No. 6,515,988). The rejection is respectfully traversed.

By the present amendment, the Applicant has amended independent claim 1 to include substantially all of the limitations of claim 9, and has also therefore cancelled claim 9. The Examiner rejected claim 9 as anticipated by Eldridge by asserting that, among other similarities, Eldridge discloses printing, at the printer, an authorization identifier and a printer identifier. The Examiner asserted that such a step is disclosed in Eldridge at col. 10, lines 3-6. However, those lines of Eldridge state merely: "*The token may include further service parameters, as discussed in Section 2 above. This enables the exact print service required (e.g. printer id, number of copies, 2-sided, etc.) to be deduced (step s133).*" The Applicant respectfully asserts that those lines do not disclose or fairly suggest printing at a printer an authorization identifier and a printer identifier.

The tokens of Eldridge are expressly described as part of system for transmitting and securing documents that may be located in remote locations far away from actual users. See, e.g., Eldridge at col. 9, lines 24-27: "*An element of this routine is the request for a document held in an electronic repository—here it is illustrated as being stored on a remote file server 52 (which may be in a different building or in a different country)....*" That is very different from the network terminal authorization method defined in the present claims that concerns access to local printers. A key concept behind the present invention—and a key limitation of the present claims that apparently has not been acknowledged by the Examiner—is that the present method enables secure access to printers by requiring a printer authorization identifier to be physically obtained at the printer itself. To further clarify that limitation, the presently amended claim 1 includes the limitation of "*providing to a user, at the printer, the authorization identifier and the printer identifier.*" That guarantees that a later user of the printer, who accesses the printer from a web terminal, must have had some form of physical access to the printer in order to obtain the secret authorization identifier—which was provided only at the printer.

The method of the present claims is thus very useful for minimizing, for example, printer spamming when a printer is accessible through the Internet. For instance, a home or business user of the present invention, who has both a local printer and a local personal computer (PC), may desire to print to the printer from the PC via the internet, i.e., without a direct connection between the PC and the printer. The method of the present invention enables such a home or business user to print an authorization identifier at the local printer and then use that identifier to gain access to the printer through the Internet. It is envisioned that physical access to the printer could be obtained by, for example, receiving a physical page printed at the printer, where the page includes the authorization identifier. Alternatively the printer could provide the authorization identifier on a display screen on the printer, or in any other manner that is understandable to a user that is in the physical vicinity of the printer.

To still further clarify the function of the present invention, claim 1 has also been amended to add the following statement to the second receiving step: "*...whereby the user of the network terminal proves physical access to the printer because the user obtained the printer identifier through physical access to the printer, thus increasing printer security.*" That should make it abundantly clear that the limitations of the presently amended claims are neither disclosed nor fairly suggested in Eldridge et al. The disclosure of Eldridge et al. does not concern the maintenance of network security through actual physical access to a network device.

Support for the present amendments to the claims may be found, for example, in the specification as filed in FIG. 51 and at page 50, lines 5-10: "*A preferred embodiment of a Web terminal authorization protocol is shown in Figure 51. According to the protocol, the onetime authorization proceeds as follows: the user requests a Web terminal authorization page via the printer 601. The netpage registrations server generates a short-lifetime one-time-use authorization ID 412 for the Web terminal which is printed on the authorization page 413, together with the URI of the printer.*"

Conclusion

Independent claim 1 has been amended to incorporate some of the limitations of original claim 9 as well as additional limitations intended to further clarify the distinctions of the present invention over the cited prior art. All of the other remaining claims are dependent on claim 1. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicant:

PAUL LAPSTUN

KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762